INFORMATION PROCESSING APPARATUS AND METHOD

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority from Japanese Application Nos. P2000-205615, filed July 6, 2000, and P2000-211787, filed July 12, 2000, the disclosures of which are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

[0002] The present invention relates to an information processing apparatus and method. More particularly, the present invention relates to an information processing apparatus and method in which use of content can be limited.

[0003] In recent years, network systems typified by the Internet have become popular. As a result, it is now possible for users to transmit or receive information via the Internet.

[0004] A user who wants to view or listen to authored material such as movies or music can pay to receive the authored material.

[0005] However, there is a risk that in addition to the owner, other people, who have not paid to receive authored material such as movies or music, may fraudulently view or listen to the authored material through a network such as the Internet.

[0006] Also, if illegal viewing or listening through a network continues unrestrained, the content creation and distribution business will suffer.

SUMMARY OF THE INVENTION

[0007] The present invention has been made in view of such circumstances. An object of the present invention is to prevent content from being illegally used via a network.

[0008] To this end, in one aspect, the present invention provides an information processing apparatus for transmitting content to another apparatus via a network. The information processing apparatus includes an encryption unit operable to encrypt the content; an authentication unit operable to perform an authentication procedure with the another apparatus

1

when the another apparatus requests permission to receive the encrypted content, the authentication procedure providing an authentication result; a transmitter operable to transmit a decryption key for decrypting the encrypted content to the another apparatus based on the authentication result; a first obtaining unit operable to obtain identification information of the another apparatus based on the authentication result; a first counting unit operable to count a total number of units desiring to receive the encrypted content based on the identification information; a storage unit operable to store the identification information of the another apparatus; and a controller operable to control a total number of units approved to receive the encrypted content based on the total number of units desiring to receive the encrypted content.

[0009]   The information processing apparatus may further include a second obtaining unit operable to obtain a number of additional units desiring to receive the encrypted content from the another apparatus based on the authentication result; and a second counting unit operable to count a total number of units of the another apparatus desiring to receive the encrypted content based on the number of additional units.

[0010]   The information processing apparatus may further include an information updating unit operable to delete the identification information stored in the storage unit and to reset the total number of units approved to receive the encrypted content when the decryption key is changed.

[0011]   In another aspect, the present invention provides a method for transmitting content from an information processing apparatus to another apparatus via a network. The method includes encrypting the content; performing an authentication procedure with the another apparatus when the another apparatus requests permission to receive´ the encrypted content, the authentication procedure producing an authentication result; transmitting a decryption key for

2

decrypting the encrypted content to the another apparatus based on the authentication result; obtaining identification information of the another apparatus based on the authentication result; counting a total number of units desiring to receive the encrypted content based on the identification information; storing the identification information of the another apparatus; and controlling a total number of units approved to receive the encrypted content based on the total number of units desiring to receive the encrypted content.

[0012] In another aspect, the present invention provides a recording medium having recorded thereon a program for transmitting content from an information processing apparatus to another apparatus in a network, the program including encrypting the content; performing an authentication procedure with the another apparatus when the another apparatus requests permission to receive the encrypted content, the authentication procedure producing an authentication result; transmitting a decryption key for decrypting the encrypted content to the another apparatus based on the authentication result; obtaining identification information of the another apparatus based on the authentication result; counting a total number of units desiring to receive the encrypted content based on the identification information; storing the identification information of the another apparatus; and controlling a total number of units approved to receive the encrypted content based on the total number of units desiring to receive the encrypted content.

[0013] In the information processing apparatus, the information processing method, and the program recorded on the recording medium, content is encrypted, and when a request for reception permission is made from another apparatus, an authentication procedure is performed with the other apparatus as long as the number of receiving units does not exceed a

3

permissible value even if the reception is permitted, and a decryption key for decrypting the encrypted content is transmitted to the other apparatus on the basis of the authentication result.

[0014] In another aspect, the present invention provides an information processing apparatus for receiving content from a first apparatus via a first network. The information processing apparatus includes a first transmitter operable to transmit to the first apparatus a request for permission to receive the content; a first authentication unit operable to perform a first authentication procedure with the first apparatus, the first authentication procedure producing a first authentication result; a receiver operable to receive from the first apparatus a first decryption key for decrypting the content based on the first authentication result; a second transmitter operable to transmit the content received from the first apparatus to a second apparatus via a second network; a second authentication unit operable to perform a second authentication procedure with the second apparatus when a request for permission to receive the content is made from the second apparatus, the second authentication procedure producing a second authentication result; a third transmitter operable to transmit a second decryption key to the second apparatus based on the second authentication result; a first obtaining unit operable to obtain identification information of the second apparatus based on the second authentication result; a first counting unit operable to count a number of units desiring to receive the content based on the identification information; a storage unit operable to store the identification information of the second apparatus; and a controller operable to control a number of units approved to receive the content based on the number of units desiring to receive the content.

4

[0015] The information processing apparatus of the present invention may further include a decryption unit operable to decrypt the content; and an encryption unit operable to encrypt the content decrypted by the decryption unit.

[0016] The information processing apparatus of the present invention may further include a fourth transmitter operable to transmit the number of units desiring to receive the content to the first apparatus based on the first authentication result; a second obtaining unit operable to obtain a number of additional units desiring to receive the content from the second apparatus based on the second authentication result; and a second counting unit operable to count a total number of units of the second apparatus desiring to receive the content based on the number of additional units.

[0017] The information processing apparatus in accordance with this aspect of the present invention may further include an information updating unit operable to delete the identification information stored in the storage unit and to reset the number of units approved to receive the content when the second decryption key is changed.

[0018] In another aspect, the present invention provides a method for receiving content in an information processing apparatus from a first apparatus via a first network. The method includes transmitting to the first apparatus a request for permission to receive the content; performing a first authentication procedure with the first apparatus to obtain a first authentication result; receiving from the first apparatus a first decryption key for decrypting the content based on the first authentication result; transmitting the content received from the first apparatus to a second apparatus via a second network; performing a second authentication procedure with the second apparatus when a request for permission to receive the content is made from the second apparatus, the second authentication procedure

5

producing a second authentication result; transmitting a second decryption key to the second apparatus based on the second authentication result; obtaining identification information of the second apparatus based on the second authentication result; counting a number of units desiring to receive the content based on the identification information; storing the identification information of the second apparatus; and controlling a number of units approved to receive the content based on the number of units desiring to receive the content.

[0019] In another aspect, the present invention provides a recording medium having recorded thereon a program for receiving content in an information processing apparatus from a first apparatus via a network. The program includes transmitting to the first apparatus a request for permission to receive the content; performing a first authentication procedure with the first apparatus to obtain a first authentication result; receiving from the first apparatus a first decryption key for decrypting the content based on the first authentication result; transmitting the content received from the first apparatus to a second apparatus via a second network; performing a second authentication procedure with the second apparatus when a request for permission to receive the content is made from the second apparatus, the second authentication procedure producing a second authentication result; transmitting a second decryption key to the second apparatus based on the second authentication result; obtaining identification information of the second apparatus based on the second authentication result; counting a number of units desiring to receive the content based on the identification information; storing the identification information of the second apparatus; and controlling a number of units approved to receive the content based on the number of units desiring to receive the content.

6

[0020] In the information processing apparatus, the information processing method, and the program recorded on the recording medium, the content received from the first apparatus via the first network is transmitted to the second apparatus via the second network with the permissible number of units obtained from the first apparatus as an upper limit.

[0021] The above and further objects, aspects and novel features of the invention will become more fully apparent from the following detailed description when read in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] Fig. 1 is a block diagram showing an example of the configuration of a network system to which the present invention is applied;

[0023] Fig. 2 is a block diagram showing a detailed example of the construction of a source of Fig. 1;

[0024] Fig. 3 is a block diagram showing a detailed example of the construction of a sink of Fig. 1;

[0025] Fig. 4 is a block diagram showing a detailed example of the construction of a bridge of Fig. 1;

[0026] Fig. 5 is an illustration of an authentication process between a source or a bridge, and a sink;

[0027] Fig. 6 is a flowchart illustrating an authentication process by the sink for a source or a bridge;

[0028] Fig. 7 is a flowchart illustrating an authentication process by a source or a bridge for a source;

[0029] Fig. 8 is a flowchart illustrating an authentication process by a source or a Tx bridge for an Rx bridge;

[0030] Fig. 9 is a flowchart illustrating an authentication process by the Rx bridge for the source or the Tx bridge; and

[0031] Fig. 10 is a flowchart illustrating an authentication process by the source or the Tx bridge for the Rx bridge.

DETAILED DESCRIPTION

[0032] Fig. 1 is a block diagram showing an example of the configuration of a network system to which the present invention is applied. In this network system, a source 1 is connected to a sink 2-1 and a bridge 3-1 via a bus 4-1. The bridge 3-1 is connected to a sink 2-2 and a bridge 3-2 via a bus 4-2. Furthermore, the bridge 3-2 is connected to sinks 2-3 and 2-4 via a bus 4-3.

[0033] The source 1 is an output device for outputting content. When content is to be output, the source 1 encrypts the content, then outputs the encrypted content to the sinks 2-1 to 2-4 via the buses 4-1 to 4-3. Key information necessary for decrypting the encrypted content is transferred only to the sink which has succeeded in an authentication process. As a result, the number of sinks which receive the content is limited. Since the bridges 3-1 and 3-2 (to be described later) only re-output a received signal, these are excluded from the object for which the number of units is counted.

[0034] Sinks 2-1 to 2-4 (hereinafter, when the sinks 2-1 to 2-4 do not need be individually identified, they are referred to simply as a "sink 2", and the same applies to other devices) are receiving units for receiving content supplied from the source 1. If a sink 2 succeeds in the authentication process, the sink 2 decrypts the received content on the basis of the key information transferred from the source 1. However, when the bridges 3-1 and 3-2 decrypt the encryption once, and encrypt with a new key and output the encrypted content, the sinks 2-2 to 2-4 decrypt the received content on the basis of the key information transferred from the bridge which is connected directly thereto.

[0035] It is assumed that the bridges 3-1 and 3-2 receive and decrypt the encrypted content which is output from the source 1, re-encrypt the content, and then output it to the

8

sinks 2-2 to 2-4. For this purpose, the bridge 3-1 performs an authentication process with the source 1, obtains key information necessary for decrypting the encrypted content, and tells the source 1 the number of sinks 2 for which the content to be re-output is desired to be received. Then, when the bridge 3-1 obtains permission from the source 1, the bridge 3-1, instead of the source 1, limits the number of sinks 2-2 to 2-4 which receive the content. The bridge 3-2 performs an authentication process with the bridge 3-1, and similarly limits the number of sinks 2-3 and 2-4 which receive the content.

[0036]   Fig. 2 is a block diagram showing a detailed example of the construction of the source 1.

[0037]   When a medium 12 is loaded, a content player 11, under the control of a control section 15, plays back the content recorded on the medium 12, and outputs the content to an encryption section 13. The encryption section 13 encrypts the content input from the content player 11, and outputs it externally via a communication interface (I/F) 14. In place of the content player 11 and the medium 12, a source having a tuner which receives and outputs broadcast content may be used.

[0038]   The control section 15 controls the content player 11, the encryption section 13, the communication I/F 14, and a storage section 16. Also, the control section 15 causes the content played back by the content player 11 to be stored in the storage section 16 as necessary.

[0039]   Fig. 3 is a block diagram showing a detailed example of the construction of a sink 2.

[0040]   A control section 24 controls an image/audio output section 21, a decryption section 22, a communication I/F 23, and a storage section 25. Also, the control section 24 sends the encrypted content, transmitted via the communication I/F 23, to the decryption section 22.

[0041]   The decryption section 22 obtains the key information transmitted from the source 1 through the communication I/F 23.   Also, the decryption section 22 decrypts the content on the basis of the obtained key information.   The image/audio output section 21 outputs the content decrypted by the decryption section 22.

[0042]   Fig. 4 is a block diagram showing a detailed example of the construction of a bridge 3.

[0043]   A control section 35 controls a communication I/F 31, a decryption section 32, an encryption section 33, a communication I/F 34, and a storage section 36.   Also, the control section 35 sends the encrypted content, transmitted via the communication I/F 31, to the decryption section 32.

[0044]   The decryption section 32 obtains the key information transmitted from the source 1 via the communication I/F 31, and decrypts the received content on the basis of the obtained key information.

[0045]   The encryption section 33 encrypts the content decrypted by the decryption section 32, and externally outputs it via the communication I/F 34.

[0046]   It is assumed that, for authentication, public-key cryptographic technology is used, and that the source 1, the sink 2, and the bridge 3 each have a digital certificate (hereinafter referred to as a "certificate"), issued by the key management organization, a secret key, and a public key of the key management organization.   It is assumed that this certificate contains a public key for each device, corresponding to the secret key for each device, the unique ID of each device, and an electronic signature for these two pieces of data supplied by the key management organization.

[0047]   Fig. 5 is an illustration of an authentication process in a case where the source 1 and the sink 2-1 (Fig. 1) are directly connected.

10

[0048] Initially, the source 1 transmits its own certificate to the sink 2-1. Specifically, the control section 15 of the source 1 reads a certificate from the storage section 16, and transmits it as a communication command to the sink 2-1 via the communication I/F 14 (① in Fig. 5).

[0049] When the sink 2-1 receives this communication command, the sink 2 determines whether or not the data is valid. Specifically, the control section 24 of the sink 2-1 checks whether or not the data in the certificate received via the communication I/F 23 corresponds to the electronic signature of the key management organization attached thereto by using the public key of the key management organization stored in the storage section 25. That is, the control section 24 determines the validity of the received data by performing a DSA (Digital Signature Algorithm) verification computation process for public key encryption. If the determination result shows that the received data is valid, the authentication process continues. Otherwise, the authentication process is terminated.

[0050] If the processing continues, the control section 15 of the source 1 checks whether or not the ID of the other party in the certificate has already been entered in the authenticated ID list (hereinafter described as an "ID list") stored in the storage section 16. If the certificate has already been entered, "0" is substituted in a variable CntUp.

[0051] If, on the other hand, the ID of the other party in the certificate has not been entered in the ID list, the control section 15 of the source 1 compares the number of sinks 2 for which reception has been permitted (hereinafter described as a "variable SinkCnt") with the upper-limit number which indicates the number of receptions which are permitted (hereinafter described as a "variable MaxSink"). When the

11

variable SinkCnt is smaller, "1" is substituted in the variable CntUp.

[0052] When SinkCnt = MaxSink, the authentication process is terminated. Also, the variable MaxSink may not be a variable (that is, it may be a constant).

[0053] Then, the control section 15 of the source 1 generates a pseudo-random number Random_challenge on the basis of a pseudo-random number generation algorithm, and transmits it as a communication command to the sink 2 (② in Fig. 5).

[0054] When the control section 24 of the sink 2-1 receives this communication command, the control section 24 performs a DSA Sign computation process for public key encryption on the value thereof by using its own secret key stored in the storage section 25 in order to calculate the electronic signature. The control section 24 of the sink 2-1 transmits the calculated electronic signature, as a communication command (Response data), to the source 1 (③ in Fig. 5).

[0055] When the control section 15 of the source 1 receives this communication command, the control section 15 determines whether or not the pseudo-random number Random_challenge transmitted by the control section 15 corresponds to this electronic signature, that is, performs the above-mentioned DSA verification computation process in order to determine the validity of the data. Here, however, in place of the above-described public key of the key management organization, the public key of the other party in the certificate received from the other party is used. When the result of the determination shows that the data is valid, the authentication process is continued. Otherwise, the authentication process is terminated.

[0056] When the processing continues, the control section 15 of the source 1 transmits to the sink 2-1, as a communication command, key information necessary for decrypting the encryption applied to the content (④ in Fig.

5), and increases the value of the variable SinkCnt by the value of the variable CntUp. Then, the control section 15 of the source 1 checks whether or not the ID of the other party in the certificate has already been entered in the authenticated ID list stored in the storage section 16. If it has already been entered, "0" is substituted in the variable CntUp. On the other hand, if the ID of the other party in the certificate has not been entered in the ID list, the variable SinkCnt is compared with the variable MaxSink, and if the variable SinkCnt is smaller, "1" is substituted in the variable CntUp.

[0057] The sink 2-1 can receive the content by receiving the key information and by decrypting the encryption applied to the content by using the key information.

[0058] Also, as in the source 1 and the sink 2-2 shown in Fig. 1, in a case where the content output from the source 1 is received by the sink 2-2 after going through the bridge 3-1, the sink 2-2 and the bridge 3-1 perform an authentication process such as that shown in Fig. 5. That is, even in a case where content is transmitted via two or more bridges as in the source 1 and the sink 2-3 or the source 1 and the sink 2-4, the source 1 and the last bridge 3-2 (the bridge which is directly connected to the sinks 2-3 and 2-4) perform similar authentication processes.

[0059] The processing flow of the sink 2 in the above authentication process is shown in Fig. 6, and the processing flow of the source 1 is shown in Fig. 7.

[0060] The authentication process of the source 1 is the same as that of the case of a sink 2 even if the other party is a bridge 3. For the authentication process of the bridge 3, the process shown in step S15 of Fig. 7 differs from that in the case of the sink 2. Specifically, when SinkCnt = MaxSink, in order to increase the value of the variable MaxSink, the bridge 3 performs an authentication process for

13

requesting reception permission from the source 1 or a bridge 3 (in the case of the example of Fig. 1, the source 1 if the bridge 3 is the bridge 3-1 and the bridge 3-1 if the bridge 3 is the bridge 3-2) which is the transmission source of the content received (input) by the bridge 3. In this case, a request for an additional increase in the number of receiving units by one or more is made. When this authentication process is successful, the processing of step S16 or subsequent steps in Fig. 7 is continued.

[0061] Fig. 8 is an illustration of an authentication process in a case where the source 1 and the bridge 3-1 (Fig. 1) are directly connected.

[0062] Initially, the control section 35 of the bridge 3-1 transmits its own certificate, variable RelCnt, and variable AbsCnt to the source 1 (① in Fig. 8). Here, the variable RelCnt represents the number of units for which the bridge 3-1 desires to newly obtain reception permission, and the variable AbsCnt represents the total number of units for which permission has already been obtained and the number of units for which permission is desired this time.

[0063] When the control section 15 of the source 1 receives the certificate and the variables, the control section 15 determines whether or not the certificate is valid by performing the above-described DSA verification computation process. When the result of the determination shows that the certificate is not valid, the authentication process is terminated.

[0064] When the processing continues, the control section 15 of the source 1 checks whether or not the ID of the other party in the certificate has already been entered in its own ID list. If the certificate has already been entered, the variable RelCnt is substituted in the variable CntUp.

[0065] If, on the other hand, the ID of the other party in the certificate has not been entered in the ID list, the

14

control section 15 of the source 1 substitutes the variable AbsCnt in the variable CntUp. Then, the control section 15 of the source 1 determines whether the value resulting when the variable CntUp is added to the variable SinkCnt is smaller than the variable MaxSink. When they are equal, the authentication process is terminated.

[0066] Then, the control section 15 of the source 1 generates a pseudo-random number Random_challenge, and transmits it as a communication command to the bridge 3-1 (② in Fig. 8).

[0067] When the control section 35 of the bridge 3-1 receives this communication command, the control section 35 performs the above-described DSA Sign computation process on that value, and the transmitted variable RelCnt and variable AbsCnt by using its own secret key stored in the storage section 36 in order to calculate the electronic signature. The control section 35 of the bridge 3-1 transmits the calculated electronic signature as a communication command (Response data) to the source 1 (③ in Fig. 8).

[0068] When the control section 15 of the source 1 receives this communication command, the control section 15 determines whether or not this electronic signature corresponds to the pseudo-random number Random_challenge transmitted by the control section 15 and the received variable RelCnt and variable AbsCnt, that is, determines the validity of the data by performing the DSA verification computation process. Here, however, in place of the above-described public key of the key management organization, the public key of the other party in the certificate received from the other party is used. When the result of the determination shows that the data is not valid, the authentication process is terminated.

[0069] When the processing continues, the control section 15 of the source 1 transmits, as a communication command, to the bridge 3-1 the key information necessary for decrypting

15

the encryption applied to the content (④ in Fig. 8), and increases the value of the variable SinkCnt by the value of the variable CntUp. After this, if the ID of the other party has not been entered in the ID list, the control section 15 adds it to the list.

[0070] The bridge 3-1 receives the key information and decrypts the encryption applied to the content by using the key information, re-encrypts the content, and then outputs it. Then, the control section 35 of the bridge 3-1 increases the value of the variable MaxSink by the value of the variable RelCnt.

[0071] The processing flow of the bridge 3 in the above authentication process is shown in Fig. 9, and the processing flow of the source 1 is shown in Fig. 10.

[0072] As in the source 1 and the sink 2-3 or the source 1 and the sink 2-4 shown in Fig. 1, in a case where the content which is output from the source 1 is received by the sinks 2-3 and 2-4 after going through two of bridges 3-1 and 3-2 or more, the bridge 3-1 which outputs the content (hereinafter described as a "Tx bridge") and the bridge 3-2 which receives it (hereinafter described as an "Rx bridge") perform an authentication process such as that shown in Fig. 8.

[0073] The authentication process of the Rx bridge is the same as that in the case where the other party is the source 1.

[0074] For the authentication process of the Tx bridge, the process shown in step S46 of Fig. 10 differs from that of the case of the source 1. Specifically, when SinkCnt + CntUp > MaxSink, in order to increase the value of the variable MaxSink, the Tx bridge performs an authentication process for requesting the source 1 or the bridge 3, which is the transmission source of the content input to the Tx bridge, to permit reception (in the case of the example of Fig. 1, the bridge 3-1 requests authentication from the source 1). In

this case, a request for additional information in the number of receiving units of ((SinkCnt + CntUp) - MaxSink) or more is made. When this authentication process is successful, the processing of step S50 and subsequent steps of Fig. 10 continues.

[0075] As another processing example, a case in which the variable RelCnt and the variable AbsCnt are transmitted separately from the certificate is possible. For example, there is also a method of transmitting them together with the Response shown at ③ in Fig. 8 or transmitting them by a completely different communication command.

[0076] Also, there is a method in which in step S15 of Fig. 7 or in step S46 of Fig. 10, when the bridges 3-1 and 3-2 perform an authentication process with a newly connected source 1 or bridge 3, regardless of the result, the processing thereafter is not continued. That is, a new authentication can be considered to be one for making subsequent authentications successful.

[0077] Furthermore, in a case where the sink 2 stops receiving its own output and loses information necessary for decrypting the encryption, the source 1 or the bridge 3 can decrease the number of the variable SinkCnt by the number corresponding to the number of sinks 2. For example, when the source 1 or the bridge 3 changes the key information for the encryption to be applied to the content, it is possible for the sink 2 to set the variable SinkCnt to 0.

[0078] As described above, since the source 1 or the bridge 3 limits the number of receiving units or sinks 2 capable of receiving output, the advantages such as those described below are obtained.

(1) It is possible for the owner of content to prevent illegal viewing and recording of the content.

17

(2) Even when a signal is re-output using a bridge, it is possible for the source to limit the number of units, including the sink which exists at the end of the bridge.

(3) Since the limitation of the number of units is performed using an ID unique to the device, even if the same sink performs authentication many times, the number of units will not be increased by mistake.

(4) Since the increase or decrease in the number of receiving units and the total number of receiving units are informed when the bridge requests reception permission from the source or another bridge, it is possible for the source and the other bridge to easily change the variable SinkCnt to a correct value in either the case where authentication with the bridge has been performed or the case where authentication with the bridge has not been performed.

[0079] Since public-key cryptographic technology is used, the device-unique ID and the requested number of units can be safely transferred to another unit, and correct number-of-devices management can be performed.

[0080] Although the above-described series of processes can be performed by hardware, these can also be performed by software. In the case where the series of processes is performed by software, programs which form the software are installed from a recording medium into a computer incorporated into dedicated hardware or, for example, into a general-purpose personal computer capable of executing various types of functions by installing various programs.

[0081] This recording medium is constructed by not only packaged media formed of a magnetic disk (including a floppy disk), an optical disk (including a CD-ROM (Compact Disk-Read Only Memory), and a DVD (Digital Versatile Disk)), a magneto-optical disk (including an MD (Mini-Disk)), or a semiconductor memory, in which programs are recorded, but also is constructed by a ROM, a hard disk, etc., in which programs are

18

stored, which is provided to a user in such a manner as to be preinstalled into a computer.

[0082] In this specification, steps which describe a program stored in a recording medium contain not only processing performed in a time-series manner along the described sequence, but also processing performed in parallel or individually although the processing is not necessarily performed in a time-series manner.

[0083] In this specification, the system represents the overall apparatus composed of plural devices.

[0084] Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. It is therefore to e understood that numerous modifications may be made to the illustrative embodiments and that other arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims.